

A METHOD OR SYSTEM FOR EXECUTING DEFERRED TRANSACTIONS

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Patent Application No.: 60/254,604, filed December 11, 2000, entitled METHOD AND SYSTEM FOR EXECUTING DEFERRED TRANSACTIONS, the entire disclosure of which is hereby incorporated by reference.

BACKGROUND OF THE INVENTION

[0002] The present invention relates to an electronic commerce system and method. In particular, the present invention relates to methods of, and systems for, conducting a transaction between a user of a remote communications device and a second party.

[0003] Mobil commerce, also known as m-commerce, is gaining greater market penetration as the use of electronic networks (such as the Internet) become more popular. Mobile commerce involves the execution of a transaction between a user of a remote communications device (e.g., a mobile communications device) and a second party, such as a merchant, a bank, a back-end settlement system (e.g., a transaction processing system of a financial institution), etc.

[0004] The general process steps associated with conducting a transaction between two parties using mobile commerce includes activating a mobile device and executing a software application suitable for conducting a transaction. A real time secure communications session is established between the mobile device and the other party over a communications channel to facilitate the transaction.

[0005] Parameters of a real time transaction are established, such as monetary amounts, account information, product and/or service identification, delivery information, etc. Often, these parameters are established via user input

to the software application. For example, the software application may facilitate the transmission of an electronic form from the other party to the mobile device over the communications channel. The electronic form may include entry fields, which correspond to the parameters of the transaction, e.g., product identification, price, delivery, etc. As the user enters information into the form, the information establishes at least some of the parameters of the transaction.

[0006] A real time transaction data structure is created by the software application, which includes the parameters of the transaction previously obtained. The real time transaction data structure may be augmented with a digital certificate suitable for authenticating the data structure as is known in the art. The real time transaction data structure and digital certificate, if any, is transferred to the other party over the communications channel. A response is received at the mobile device from the other party and additional steps necessary to complete the transaction are performed.

[0007] The above described conventional process for conducting a mobile transaction suffers from a substantial disadvantage in that no progress can be made in facilitating the transaction when the secure communications session over the communications channel is not established. Indeed, there are often times when the mobile device is not in communication with the other party and such communication cannot be established, for example, due to failures in certain equipment, excessive loads over the communications channel, etc. Thus, the user must wait until a later time to execute the steps necessary to conduct a transaction, despite that the present time is most convenient.

[0008] Accordingly, there is a need in the art for new methods of, and systems for, conducting a transaction

between a user of a remote communications device and a second party such that at least some of the steps in conducting the transaction may be executed despite a temporary absence of, or capability of establishing, communication between the remote communications device and the second party.

SUMMARY OF THE INVENTION

[0009] A method of conducting a transaction between a user of a remote communications device and a second party according to one aspect of the present invention includes: creating a transaction data structure based on input from the user that defines the transaction; creating a deferred transaction data structure, corresponding to the transaction data structure that defines a deferred transaction, when establishing communication between the remote communications device and the second party is temporarily not obtainable or is interrupted; storing the deferred transaction data structure in a memory; establishing communication between the remote communications device and the second party; and transmitting the deferred transaction data structure to the second party when the communication between the remote communications device and the second party is established. Preferably, the deferred transaction data structure is automatically transmitted to the second party when communication is established.

[0010] Preferably, the method further includes: creating a real time transaction data structure based on input from the user that defines a real time transaction after the deferred transaction data structure is stored in the memory; creating a combined transaction data structure by aggregating the real time transaction data structure and the deferred transaction data structure; and transmitting the combined transaction data structure to the second party.

[0011] The method may also include: establishing a digital certificate and associating the digital certificate with the transaction data structure, the digital certificate identifying the transaction, the user, and/or the remote communications device as being authorized; and associating the digital certificate with the deferred transaction data structure when establishing communication between the remote communications device and the second party is delayed.

[0012] Preferably, the method includes: assigning a transaction identification field to each transaction data structure prior to transmitting the combined transaction data structure to the second party; and/or receiving combined response data from the second party containing transaction results concerning the real time transaction data structure and the deferred transaction data structure. The method may also include parsing the combined response data and matching the respective transaction results with the real time transaction and the deferred transaction based on the transaction identification fields. Preferably, the transaction result concerning the real time transaction data structure is matched with the real time transaction before the transaction result concerning the deferred transaction data structure is matched with the deferred transaction.

[0013] The method may also preferably include assigning an application identification field to each deferred transaction data structure prior to storing the deferred transaction data structure in memory. In this situation, at least one software application is employed in creating the real time transaction data structure and the deferred transaction data structure. Preferably, the application identification field(s) are removed from each deferred transaction data structure prior to transmitting the combined transaction data structure to the second party.

[0014] Preferably, the method includes: matching the transaction result concerning the real time transaction data structure with the at least one software application to facilitate completion of the real time transaction; and/or matching the transaction result concerning the deferred transaction data structure with the at least one software application and executing the at least one software application to facilitate completion of the deferred transaction.

[0015] Alternatively, the method need not include the creation of a real time transaction or a real time transaction data structure. In this case, the above steps concerning the deferred transaction and deferred transaction data structure(s) are carried out irrespective of a real time transaction.

[0016] Preferably, at least one software application is employed in creating the deferred transaction data structure and establishing the digital certificate. In this case, it is preferred that the method include storing the digital certificate in memory when (i) establishing communication between the remote communications device and the second party is delayed and (ii) the digital certificate is an application specific digital certificate. The method may also include storing a pointer to the digital certificate in memory when (i) establishing communication between the remote communications device and the second party is delayed, and (ii) the digital certificate is a general digital certificate. Still further, the method may also include storing the digital certificate in memory (or storing a pointer to the digital certificate in memory) when (i) establishing communication between the remote communications device and the second party is delayed, and (ii) the digital certificate is specific to the remote communications device.

[0017] In accordance with another aspect of the present invention, a storage medium containing a software program capable of causing a remote communications device to execute actions in conducting a transaction between a user of the remote communications device and a second party is contemplated. Preferably, the actions include those recited in the methods hereinabove. According to still another aspect of the present invention, a remote communications device including a microprocessor operating under the control of the software program is contemplated.

[0018] Other objects, features, and advantages of the present invention will become apparent to those skilled in the art from the following description of the invention with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] For the purpose of illustrating the invention, there are shown in the drawing forms, which are presently preferred, it being understood, however, that the invention is not limited to the precise arrangements and instrumentalities shown.

[0020] FIG. 1 is a block diagram illustrating an apparatus for conducting a transaction between a user of a remote communications device and a second party in accordance with one or more aspects of the present invention;

[0021] FIG. 2 is a block diagram of a preferred remote communications device operable to conduct a transaction between a user of the remote communications device and a second party in accordance with one or more aspects of the present invention; and

[0022] FIGS. 3a, 3b, and 3c are flow diagrams illustrating process steps that may be carried out in

accordance with one or more aspects of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0023] Referring now to the drawings wherein like numerals indicate like elements, there is shown in FIG. 1 a block diagram illustrating a system 10 for carrying out a transaction between a user of a remote communications device 100, such as a mobile device, and a second party 14, such as one or more back-end settlement systems 16, a merchant, a bank, a financial institution, another person, another entity at least partially assisting in the transaction (e.g., an autonomous entity, an Internet appliance, etc.) 18. In accordance with an aspect of the invention, the remote communications device 100 includes a deferred transactions function. Communications between the remote communications device 100 and the second party 14 is facilitated over a communications channel 120, such as an electronic network, radio channel, etc. The back-end settlement system 16 may require communication with a third party financial institution 19, such as a payor bank (for the user), etc. This communication may be facilitated over communications channel 122 (which may be the same as channel 120).

[0024] Reference is now made to FIG. 2, which is a block diagram of a preferred remote communications device 100 in accordance with one or more aspects of the present invention. Preferably, the remote communications device 100 is in the form of a mobile device, such as a personal digital assistance (PDA) unit (e.g., a palm device/computer such as the Palm PilotTM, Windows CETM etc.); a cell phone (including an Internet enabled cell phone); a hand held computer (possibly including a wireless modem); a lap top computer; etc. Although mobile devices are preferred,

traditionally non-mobile communications devices are also contemplated by the invention, including personal computers, set-top boxes, telephones, etc.

[0025] The remote communications device 100 includes at least one application 102, a transaction manager 104, a communications manager 106, a deferred transactions database 108, and a digital certificate database 110. The remote communications device 100 may alternatively further include an e-business agents manager 112, and an agent database 114. For the purposes of discussion, the elements of the remote communications device 100 are illustrated as functional units, which units may be implemented in hardware, software and/or a combination of both. In one embodiment, the remote communications device 100 includes a microprocessor (not shown) operating under the control of a software program, or software programs, capable of causing the device 100 to execute actions in conducting a transaction between a user of the remote communications device 100 and a second party over a communications channel 120. Some of the functional units are preferably substantially all software, such as the application(s) 102, while other functional units may be implemented in substantially all hardware or a combination of software and hardware, such as the transaction manager 104.

[0026] An application 102 may be any user application employed to carry out a transaction, such as a web browser program that supports e-commerce transactions and/or m-commerce (e.g., retail/wholesale purchases, Internet banking, settlement transactions, Internet investment transactions, electronic data interchange transactions, etc.). The transaction manager 104 is in communication with the application 102, the deferred transactions database 108, and the communications manager 106 in a way which facilitates the transaction. The transaction is preferably

10014960.121101
a secure transaction utilizing PKI technology (e.g., including encryption/decryption, establishment of a secure communications session, verification of the second party or server-side entity, authentication of the user of the remote communications device 100, creation of digital signatures, etc.).

[0027] The communications manager 106 is preferably operable to establish and manage a communications session with an outside entity (second party) 14, such as a back-end settlement system 16, a merchant, a bank, a financial institution, another person, another entity, etc. 18 (as shown and discussed above with respect to FIG. 1). Preferably, the communications manager 106 is capable of establishing and managing any type of communications, such as cellular transmissions, Blue Tooth RF transmissions, Ethernet transmissions, Internet TCP/IP transmissions, etc.

[0028] The types of transactions contemplated by the invention include: (i) electronic network banking (e.g., funds transfers between financial accounts); (ii) settlement activities (e.g., funds clearing between financial accounts, financial institutions, etc.); (iii) retail and/or wholesale purchase and/or delivery of products or services (e.g., e-commerce transactions); (iv) electronic network investment transactions (e.g., retail and/or institutional securities, or bond, transactions); and/or (v) electronic network data interchange (e.g., exchange of information between people or institutions).

[0029] The deferred transactions database 108 is preferably operable to receive, and return, deferred transactions data structures from, and to, the transaction manager 104. The deferred transactions database 108 may also communicate with a digital certificate database 110 under certain circumstances (discussed further below).

10044960-124404

[0030] With further reference to FIGS. 3a and 3b, the process steps for carrying out the invention will now be described in conjunction with reference to the system 10 of FIG. 1 and to the remote communications device 100 of FIG. 2. At action 200, the user of the remote communications device 100 activates the device and runs one or more transaction applications 102. At action 202, the transaction manager 104 (possibly in combination with the application 102) authenticates the user in possession of the remote communications device 100, for example, via personal identification number (PIN) entry, biometric information entry (e.g., fingerprint recognition), etc. Additional details concerning the use of fingerprint recognition and/or biometric information entry in general may be found in co-pending Patent Application Number 09/510,811, entitled METHOD OF USING PERSONAL DEVICE WITH INTERNAL BIOMETRIC IN CONDUCTING TRANSACTIONS OVER A NETWORK, and filed February 23, 2000. This co-pending application is assigned to the assignee of the present application and is hereby incorporated herein in its entirety.

[0031] At action 204, an attempt to establish a communications session (preferably a secure communications session) with a second party is made. This may preferably be achieved utilizing the communications manager 106. If a secure communications session can be established, then at action 206 the process flow branches to action 208 (shown passing through action 207, which is discussed further below) where a real time transaction is executed, for example, utilizing the application 102. This involves establishing a transaction data structure, which may include monetary amounts, account numbers, financial institution data, product and/or service information, purchase amount, delivery instructions, remittance information, etc. The transaction data structure may be established by way of user

input, information stored within the remote communications device 100, and/or information obtained over the communications channel 120 from the second party 14.

[0032] If a secure communications session cannot be established at action 206, or if a secure communications session is interrupted (e.g., action 207 due to failure of the remote communications device 100 or some external cause), then the process flow branches to action 210 where a deferred transaction data structure is created from a transaction data structure. This may be achieved utilizing some or all of the information that would be included in a real time transaction data structure, it being preferred that the deferred transaction data structure contains all of the information of a real time transaction data structure augmented with an application identification field. The application identification field preferably identifies which of a plurality of applications 102 the user was executing at the time of establishing the transaction data structure and the deferred transaction data structure.

[0033] At action 214, the deferred transaction data structure is stored in a memory, preferably the deferred transactions database 108 (FIG. 2), by way of transaction manager 104. The process flow then preferably advances to action 215. It is noted that the deferred transaction data structure is preferably stored in a secure, interim memory location in the remote communications device 100 such that any attempts at tampering with the deferred transaction data structure is prevented. Advantageously, in the event that a secured communications session is temporarily not obtainable or is interrupted, the deferred transaction data structure is safe in the interim memory (e.g., the deferred transactions database 108) until it is needed. As an added level of security, the deferred transaction data structure is preferably encrypted using known PKI technology prior to

storing it in the interim memory. The transaction manager 104 may contain the necessary functionality to accomplish the encryption.

[0034] It is noted that a digital certificate may be created at the time that a transaction data structure is created, which digital certificate is capable of authenticating the user, the transaction data structure, and/or the remote communications device 100 itself, thereby ensuring that the transaction is authorized. When a digital certificate is created, it is preferred that the digital certificate be stored with the deferred transaction data structure, for example, in the deferred transactions database 108. When the digital certificate is an application specific digital certificate (i.e., a digital certificate which is utilized by only one application 102, or only certain applications 102), then the digital certificate is preferably stored in the deferred transactions database 108. When the digital certificate is a general digital certificate (i.e., a digital certificate utilized by substantially all of the applications 102), then the digital certificate is preferably stored in a digital certificate database 110 (FIG. 2) such that it may be accessed by any or all of the applications 102. When the digital certificate is specific to the remote communications device 100 (i.e., a digital certificate that authenticates the remote communications device 100 itself), then the digital certificate is preferably stored in the digital certificate database 110. It is noted that the digital certificate could also be a device independent (i.e., transportable) digital certificate. When a digital certificate is stored in the digital certificate database 110, a pointer is preferably stored with the deferred transaction data structure that points to the digital certificate stored in the digital certificate database 110.

10014960-121101

[0035] At action 215, each of the transaction applications 102 are preferably notified that a corresponding deferred transaction has been (or is being) created. A reference to the deferred transaction data structure of the corresponding deferred transaction is also preferably provided to the transaction application 102, such as a unique identification number, etc. Advantageously, this notification and access to the deferred transaction data structure provides the transaction application with an opportunity to execute appropriate actions in response to the unexpected deferred transaction, such as clean-up etc.

[0036] Advantageously, the user is capable of making progress concerning a transaction (i.e., creating a deferred transaction data structure) despite that a secure communications session could not be established with the second party at actions 204, 206, or a secure communications session was lost (action 207). Thus, the user need not expend the effort necessary in creating a real time transaction data structure in the future to facilitate a transaction, which may be defined by the deferred transaction data structure in the present. Indeed, the deferred transaction data structure will be accessible (either automatically or via user command) at a future time when a secure communications session can be established.

[0037] Turning again to actions 204, 206, at some time in the future, communications (preferably secure communications) is established between the remote communications device 100 and the second party, for example, a merchant. At action 208, the user preferably executes a real time transaction by creating a transaction data structure defining the real time transaction. It is noted that a real time transaction need not be executed to fall within the scope of the invention. Indeed, the user may wish only to execute one or more of the deferred

transactions. Either automatically, or at the user's command, the deferred transactions database 108 is searched for deferred transaction data structure(s) (action 210A). At action 212A, if no deferred transaction data structure(s) exist, then the process flow branches to action 222 (FIG. 3b). If such deferred transaction data structure(s) exist, then the process flow branches to action 214A where the application identification field is preferably removed from each deferred transaction data structure.

[0038] At action 216A, a transaction identification field is preferably added to each transaction, for example, the real time transaction, if any, may be assigned an identification field of one (1), a first deferred transaction may be assigned an identification field of two (2), etc. At action 218, (FIG. 3b) any digital certificates that were stored in the digital certificate database 110 are restored. Alternatively, if the digital certificates were stored in the deferred transactions database 108, then they are preferably restored when the deferred transaction data structures are read out of the deferred transactions database 108, for example, at actions 210, 212.

[0039] At action 220, a combined transaction data structure is preferably created containing the real time, if any, and one or more deferred transaction data structures. As was discussed above, it is preferred that the deferred transaction data structure is stored in encrypted form. It is also preferred that the combined transaction data structure include the deferred transaction data structures in such encrypted form. At action 222, the combined transaction data structure is transmitted using the communications manager 106 over the communications channel 120 to the second party. It is noted that the combined transaction data structure would contain only the real time transaction data structure, if any, if no deferred

transaction data structure(s) exist. Likewise, if no real time transaction data structure exists, then the combined transaction data structure would contain only one or more deferred transaction data structures.

[0040] At action 224, the second party preferably parses the combined transaction data structure to determine the number of separate transactions contained therein. If the combined transaction data structure contained encrypted transaction data structures, then the second party would first decrypt the transaction data structures. Each transaction data structure is then processed in a manner well known in the art, for example, by communicating with at least one third party, e.g., merchants, banks, etc. If such communication requires the transmission of the transaction data structure(s), then encryption/decryption is preferably employed to maintain security. The second party preferably prepares response data containing transaction results for each of the transactions of the combined transaction data structure (action 226). The response data is then transmitted to the remote communications device 100 over the communications channel 120. Preferably, the transaction results are encrypted (individually or collectively) prior to transmission over the communications channel 120.

[0041] At action 228, the remote communications device 100 preferably parses the response data and matches any separate transaction results to the separate transactions and associated applications 102. This is preferably accomplished using the transaction identification fields and application identification fields. If the transaction results were encrypted prior to transmission, then the transaction manager 104 preferably decrypts them prior to parsing the response data. Preferably, the real time transaction result, if any, is matched with the real time transaction first. At action 230, the associated

applications 102 may be executed such that they may draw upon the information in the respective transaction results and the transaction may be completed. It is noted that underlying software services layers (which are substantially transparent to the user) may draw upon the transaction results as well as the associated applications 102 (which are user-level layers).

[0042] In accordance with an alternative embodiment of the present invention, and with reference to FIGS. 3a and 3b, if a deferred transaction data structure exists (action 212A), then the process flow preferably branches to action 240 (FIG. 3c). There, the transaction application 102 corresponding to the deferred transaction data structure is preferably identified and, at action 242, that transaction application 102 is preferably executed. At action 244, the information contained in the deferred transaction data structure is preferably utilized to facilitate the action of a real time transaction. Thus, the second party 14 (e.g., a back-end settlement system 16) need not have the capabilities of determining whether a transaction is real time or deferred. Instead, the remote communications device 100 is operable to transmit the information contained in the deferred transaction data structure to the back-end settlement system 16 in a way that the back-end settlement system 16 would treat as a real time transaction. For example, this may involve transmitting the entire transaction data structure to the back-end settlement system 16 (action 246).

[0043] At action 248, the remote communications device 100 preferably receives response data from the back-end settlement system 16 and, at action 250, matches the transaction results to the corresponding transaction and associated transaction application 102. At action 252, the associated transaction application 102 may draw upon the

information in the transaction results and the transaction may be completed.

[0044] According to at least one aspect of the invention, the remote communications device 100 preferably includes a microprocessor operating under the control of a software program. The software program is preferably capable of causing the remote communications device 100 to execute the actions disclosed above in, for example, FIGS. 3a, 3b, and/or 3c. In accordance with one or more further aspects of the invention, a storage medium, such as a disk, a CD-ROM, etc. may contain the software program and may be coupled with the remote communication's device 100 in order to facilitate execution of these actions. Accordingly, the features of the invention may be advantageously implemented on existing remote communications devices by distributing the software program contained on the storage medium.

[0045] Advantageously, in accordance with the invention, the user can queue transactions (preferably secure transactions) at a convenient time such that they may be carried out transparently, immediately or at a later time. For example, ATM transactions, such as transferring money between accounts, require a significant amount of time to compose and execute at a machine location. Utilizing the invention, however, the user can queue up all of his or her transactions prior to interfacing with an ATM machine such that they may be carried out substantially simultaneously at the ATM machine. Alternatively, the user may employ the remote communications device 100 (e.g., a digital wallet) at a grocery store POS terminal to conduct a real time purchase and simultaneously execute any deferred transactions.

[0046] Security loopholes are ameliorated inasmuch as the invention supports security and user authentication at the time of transaction creation and utilizes a secure real time connection to complete the deferred transaction.

10014960.124404

[0047] The invention also permits maximization of infrastructure efficiency in communication connection and usage while reducing the transaction operation cost on a per transaction basis. Further, if a separate party supplies the infrastructure for the communications connection, that party may be provided with a small service fee when deferred transactions are carried out during a communications session. For example, a grocery store may receive a certain monetary amount for each additional deferred transaction that is not augmented with the grocery store's transaction data structures. This fee would preferably be included in the overall transaction processing fees charged by a back-end settlement system as opposed to being charged to the user.

[0048] In accordance with still one or more further aspects of the invention, additional advantages may be obtained when so-called e-business agents are incorporated into the remote communications device 100 (see FIG. 2). An e-business agent manager 112 is preferably incorporated into the system such that it monitors the activities of the applications 102, transaction manager 104, etc. and stores such monitored information in an agent database 114. In particular, outgoing transaction requests from the application 102 to the transaction manager 104 and the incoming responses from the second party 14 through the communications manager 106 are preferably captured. Data mining may be adjusted based on the deferred transactions and/or transaction results.

[0049] Although the invention herein has been described with reference to particular embodiments, it is to be understood that these embodiments are merely illustrative of the principles and applications of the present invention. It is therefore to be understood that numerous modifications may be made to the illustrative embodiments and that other

arrangements may be devised without departing from the spirit and scope of the present invention as defined by the appended claims.

10014960-124104